

**Personal Identity Verification Alternate  
(AltLinc) PIV-I  
Business Processes,  
Policies and Procedures**

Prepared for



**United States Department of Agriculture  
Office of Homeland Security (OHS)  
1400 Independence Ave, SW  
Whitten Bldg, Suite 12B  
Washington, DC 20250**

**Version 3.1**

**September 19, 2019**

### Revision Information

Version	Date	Revision Notes
1.0	12/05/2017	Initial Draft by AltLinc PIV-I Business Process Team
2.0	09/30/2018	Updated AltLinc PIV-I use cases and expiration date policy
3.0	08/01/2019	Updated AltLinc PIV-I uses cases and expiration date policy
3.1	09/19/2019	<ul style="list-style-type: none"><li>• Updated for 508 compliance</li><li>• Updated background investigation details:<ul style="list-style-type: none"><li>○ Added Tier-1 (Low Risk) anywhere NACI is referenced as they are one in the same.</li><li>○ Added in clarification on the age of an existing FBI FP check that can be used (i.e. existing FBI FP checks can be leveraged if they are no more than 120 days old)\</li></ul></li></ul>

# Table of Contents

1	Introduction .....	1
1.1	Purpose .....	1
1.2	Background .....	1
1.2.1	HSPD-12 .....	1
1.2.2	AltLinc.....	1
1.2.3	AltLinc PIV-I Use Cases.....	2
1.3	USAccess MSO PIV-I Solution.....	3
1.3.1	Card Characteristics .....	3
1.3.2	PIV-I Card Functionality.....	3
1.3.3	PIV-I Card Topology.....	3
2	AltLinc PIV-I Business Processes and Policies .....	5
2.1	AltLinc PIV-I Business Processes and Role Holders.....	5
2.1.1	Role Hierarchy.....	5
2.2	PIV-I Policies.....	5
2.2.1	AltLinc PIV-I Expiration.....	5
2.2.2	AltLinc Risk Assessment.....	5
2.2.3	Required AltLinc Onboarding Documentation.....	6
Appendix A	Definitions and Acronyms.....	1
A-1	– Definitions.....	A-1
A-2	- Acronyms.....	A-5
Appendix B	Acceptable Enrollment ID List.....	B-1

## List of Tables

TABLE 1: USDA CREDENTIAL MATRIX .....	6
TABLE 2: DEFINITIONS .....	A-1
TABLE 3: ACRONYMS .....	A-5

## LIST OF FIGURES

FIGURE 1 - ALTLINC PIV-I TOPOLOGY – CARD FRONT.....	3
FIGURE 2 - ALTLINC PIV-I TOPOLOGY – CARD BACK .....	4
FIGURE 3: ACCEPTABLE ENROLLMENT ID LIST .....	B-1

# 1 Introduction

## 1.1 Purpose

This document serves as an introduction and guide to USDA's implementation of an AltLinc Business Process and Credentialing System for the United States Department of Agriculture (USDA). The defined AltLinc business process is modeled after the Homeland Security Presidential Directive 12 (HSPD-12) LincPass business process including identity establishment and eligibility, sponsorship & enrollment, adjudication, issuance, activation and credential usage of the AltLinc credential. This document describes the roles and phases necessary to issue an AltLinc credential and provides individual business process workflows for each phase of the process.

## 1.2 Background

### 1.2.1 HSPD-12

HSPD-12 mandates all Federal departments to implement a single, standard credential for access to both physical and logical assets. Based upon this directive, the National Institute for Standards and Technology (NIST) developed FIPS 201 including a description of the minimum requirements for a Federal personal identification verification (PIV) system. USDA's HSPD-12 compliant ID is called the LincPass, as it is designed to link a person's identity to an ID credential and the credential to a person's ability to physically and logically access federally controlled buildings and information systems, respectively. USDA has made progress towards full compliance with this mandate by credentialing approximately the majority of its total applicable Federal employee population and is now undertaking the compliance for non-Federal employees (including contractors) through its participation with the General Services Administration (GSA) HSPD-12 Managed Services Office (MSO).

### 1.2.2 AltLinc

USDA's limited capability to credential its short-term employee population requires the use of an alternative credential to the USDA LincPass. Due to increased costs of provided services USDA would benefit from the PIV-I credential managed by the MSO.

USDA developed a limited version of a non-PIV AltLinc credential that had Microsoft certificates. However, due to its limited capabilities and its associated costs, USDA has sunset the program as of September 2017. USDA made the decision to transition from the non-PIV AltLinc to the PIV-I version of the AltLinc credential based on an alternatives analysis that was conducted in late 2016 which compared various alternatives to the non-PIV version of the AltLinc credential. This analysis portrayed the organizational efficiency, risk mitigation, accountability, and potential cost reductions that would benefit USDA if USDA were to transition the solution to the GSA MSO PIV-I credential. The alternatives compared included USDA's baseline requirements for a two factor credential that would support USDA policy for credentialing short-term Federal Employees/ non-Federal Employees for logical/ physical access that would not be issued a LincPass:

- A short-term, two-factor credential for those unable to obtain a BI in a timely manner
  - Must be more secure than username and password

- Can be issued to individuals working with USDA for 6 months or less (\*Note: subsequent sponsorships for AltLinc credentials are allowed from year to year. However, a person may not exceed having an AltLinc credential for more than 180 days in a single calendar year.)
- Can be issued quickly and efficiently
  - Printed/ shipped within 2 days of Sponsorship
- Cost effective when compared to the LincPass
- Provides both PACS and LACS capabilities
- Follows existing credentialing processes established by HSPD-12

Based on this decision, USDA will be moving forward with implementing the PIV-I credential and will call it AltLinc once established and available to agencies.

An AltLinc credential may be issued to short-term Federal Employees/ non-Federal Employees assigned to or associated with the agencies requiring limited access to federally controlled facilities and/or information systems for six months. Agencies may issue a subsequent AltLinc credential following a prior work termination if subsequent work terms comply with AltLinc policy (i.e. 6 months or less work term, limited Logical/ Physical access needs). In addition, AltLinc policy states that a person may not exceed having an AltLinc credential for more than 180 days in a single calendar year. In this case, the Applicant would need to be issued a LincPass credential.

The credential will have an expiration date of 6 months to facilitate financial savings and operational continuity and remain compliant with HSPD-12 policy. This credential will be a token to allow both logical and physical access and requires a favorable fingerprint adjudication.

### **1.2.3 AltLinc PIV-I Use Cases**

The policies, processes and procedures defined in this document currently support the following use cases for issuing an AltLinc credential:

- Affiliates not required per OMB M-05-24 to undergo NACI/ Tier-1 (Low Risk) – this user community requires a PIV-like credential for physical and logical access, but since they will not undergo the NACI/ Tier-1 (Low Risk) investigation, they will not qualify for a PIV credential.
- Volunteers - this user community (i.e. tour guide) has no basis to undergo a NACI/ Tier-1 (Low Risk) investigation but has physical and logical access requirements.
- Interns - this user community is not intended to be employed for enough time to justify a NACI/ Tier-1 (Low Risk) investigation or for more than the six (6) months required by OMB M-05-24 for PIV issuance, but has physical and logical access requirements.
- Seasonal Employees - this user community is not intended to be employed for enough time to justify a NACI/ Tier-1 (Low Risk) investigation or for more than the six (6) months required by OMB M-05-24 for PIV issuance, but has physical and logical access requirements.
- Temporary Employees - this user community is not intended to be employed for enough time to justify a NACI/ Tier-1 (Low Risk) investigation or for more than the six (6) months required by OMB M-05-24 for PIV issuance, but has physical and logical access requirements.
- Intermittent Employees – this user community involves individuals who work for limited time-periods at varying times and require limited logical and/ or physical access. This includes both temporary and permanent intermittent employees. Due to their short working time-periods, they may qualify for an AltLinc card if these periods are 6 months or less.

### 1.3 USAccess MSO PIV-I Solution

#### 1.3.1 Card Characteristics

The MSO PIV-I credential meets the PIV technical specifications to work with Federal PIV infrastructure elements such as card readers, and is issued in a manner that allows Federal Government Relying Parties to trust the card.

- The PIV-I Card is suitable for level of assurance 4 as defined in OMB Memorandum M-04-04 and NIST SP 800-63, as well as multi-factor authentication as defined in NIST SP 800-116
- Configurable card expiration (agency based) for up to 5 years – USDA’s policy is 6 months
- Requires a fingerprint check (NCHC)
- Does not require a NACI/ Tier-1 (Low Risk)
- Able to be issued by Non-Federal Issuers (NFI) and accepted by the Federal Government

#### 1.3.2 PIV-I Card Functionality

The PIV-I card uses the same cardstock as the PIV card. It has a chip that allows for physical and logical access. The certificates on the card are issued from a Non-Federal Issuer Certificate Authority and are electronically distinguishable from a PIV card.

#### 1.3.3 PIV-I Card Topology

The PIV-I cards are visually different from a PIV card as shown below. PIV-I credential orientation is landscape vs. portrait orientation of PIV.

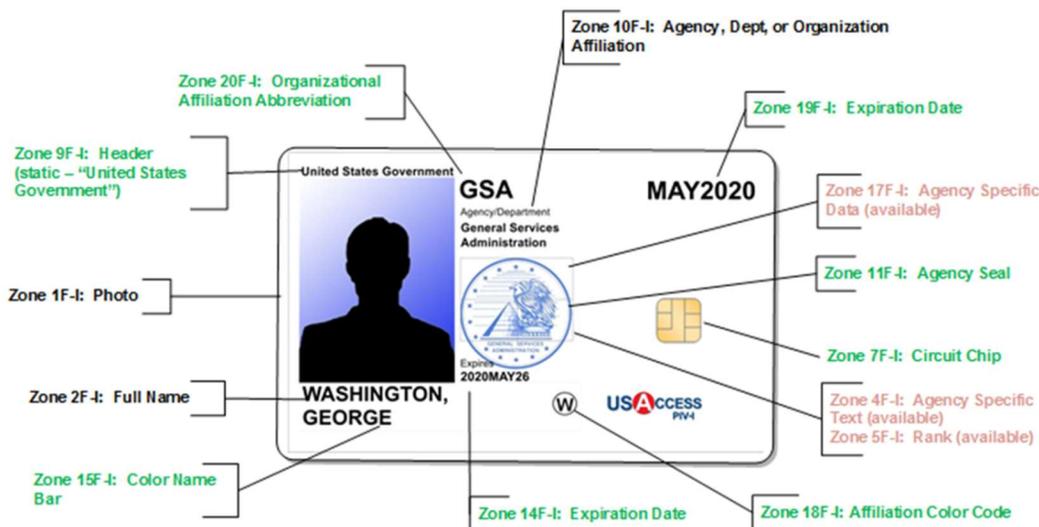


Figure 1 - AltLinc PIV-I Topology – Card Front



Figure 2 - AltLinc PIV-I Topology – Card Back

## 2 AltLinc PIV-I Business Processes and Policies

### 2.1 AltLinc PIV-I Business Processes and Role Holders

The MSO PIV-I credential has been integrated seamlessly into the USAccess system utilizing the same business processes and role holder requirements as the MSO PIV credential. Due to USDA's existing integration with the USAccess system for the LincPass, USDA will leverage the existing processes for AltLinc PIV-I issuance. Therefore, it is recommended that USDA agencies leverage existing HSPD-12 processes, role-holders and role-holder administration hierarchy policy, which maintains each Agencies' cardholders and access privileges. These responsibilities include the following activities as related to site badges for identification and facility access purposes:

- Verification of Identity Data
- Sponsorship and Enrollment
- Adjudication
- Badge Issuance, Activation and Maintenance
- Management of facility access rights
- Credential Suspension and Revocation

This will allow USDA to seamlessly continue to manage the chain of trust established in functional processes, as well as appropriate privacy and security controls using the same roles for both PIV and PIV-I issuance.

#### 2.1.1 Role Hierarchy

The AltLinc PIV-I role hierarchy is the same as the existing HSPD-12 role hierarchy. The USDA Role Administrator must have a LincPass in order to manage the AltLinc Role Hierarchy.

## 2.2 PIV-I Policies

### 2.2.1 AltLinc PIV-I Expiration

USDA's AltLinc PIV-I credential will have an expiration date of 6 months. HSPD-12 sponsors should sponsor qualifying personnel within USDA's authoritative HR system(s) (Person Model/ EmpowHR). The backend system will configure the expiration date printed on the credential accordingly based on policy. \*\*Please note that expiration dates will be printed based on 6 months from the date of sponsorship + 1 month to accommodate time for accommodating adjudication, printing and shipping the card (i.e. total of 7 months from sponsorship date).

### 2.2.2 AltLinc Risk Assessment

The USDA Credential Matrix/ Risk Assessment below illustrates the regulations that determine the type of credential that a Federal Employee/ Non-Federal Employee will be required to have. This credential

matrix should be used to determine if a Federal Employee/ Non-Federal Employee requires an AltLinc PIV-I, a LincPass, Site Badge, Visitor Badge or no credential.

**USDA Credential Matrix**

ACCESS RIGHTS	LINC PASS	ALTLINC	SITE BADGE	VISITOR BADGE	NO BADGE
RESTRICTED IT (REGARDLESS OF ANY OTHER ACCESS OR TERM OF EMPLOYMENT)	✓				
RESTRICTED PHYSICAL (REGARDLESS OF ANY OTHER ACCESS OR TERM OF EMPLOYMENT)	✓				
LIMITED IT / LIMITED PHYSICAL < 6 MONTHS (BADGE DETERMINED BY AGENCY)*		✓			
LIMITED IT / LIMITED PHYSICAL > 6 MONTHS (BADGE DETERMINED BY AGENCY)	✓				
LIMITED IT / NO PHYSICAL < 6 MONTHS (WORK OFF-SITE)*		✓			
LIMITED IT / NO PHYSICAL > 6 MONTHS	✓				
NO IT / LIMITED PHYSICAL < 6 MONTHS*		✓			
NO IT / LIMITED PHYSICAL > 6 MONTHS	✓				
NO IT / UNACCOMPANIED PHYSICAL ACCESS			✓		
NO IT / ACCOMPANIED PHYSICAL ACCESS				✓	
NO IT / NO PHYSICAL					✓

\* For individuals who require access rights for less than 6 months, this is an agency determination that is dependent on access to systems and/ or facilities.

ACCESS TYPE	ACCESS DESCRIPTION
RESTRICTED IT ACCESS	✓ ELEVATED PRIVILEGES FOR SENSITIVE OR MISSION CRITICAL APPLICATIONS
	✓ ACCESS TO APPLICATIONS BEYOND THOSE CONSIDERED LIMITED
LIMITED IT ACCESS	✓ ACCESS LIMITED TO ONLY USDA EMAIL, T&A APPLICATION, AGLearn, & GOVTRIP
RESTRICTED PHYSICAL ACCESS	✓ UNACCOMPANIED ACCESS TO USDA FACILITIES
LIMITED PHYSICAL ACCESS	✓ UNACCOMPANIED ACCESS TO GENERAL COMMON AREAS AND WORKSPACE ONLY

Table 1: USDA Credential Matrix

**2.2.3 Required AltLinc Onboarding Documentation**

In order to obtain an AltLinc PIV-I credential, the following should be required during the onboarding process:

1. OF-306
2. I-9 Documents – approved documents are included in Appendix B
3. e-Verify (this only needs to be performed one time; for subsequent sponsorships, the original e-Verify check will be adequate)
4. FBI Fingerprint Check
5. Personally Identifiable Information (required for creating identity in Human Resources System)

The following information in this section provides additional detail on the requirements related to the above onboarding documentation.

NOTE: There is an exception to AltLinc PIV-I requirements for UNPAID (i.e. volunteers and interns) individuals who qualify for an AltLinc PIV-I card (based on the requirements in the USDA credential matrix). These individuals WILL NOT have to complete an I-9 form or have an e-Verify check

completed. Instead, they just need to have a completed OF-306, a valid ID check, and an FBI fingerprint check.

### 2.2.3.1 OMB Approved Forms

To comply with the Paperwork Reduction Act (PRA) of 1995, all agencies will be required to use OMB approved forms throughout the identity proofing and registration process. Most of these forms are standard Federal government-wide forms that have been available for many years. In addition to the government-wide forms, the USDA has created an additional PIV specific form that will fulfill the information gathering requirements of the PIV program. The following is a list of approved forms for use in the AltLinc process:

- OF-306 – This form must be reviewed and stored in the Applicant’s OPF if the Applicant is a Federal Employee and properly stored by the by the Applicant’s HR/ Security representative if the Applicant is a Non-Federal Employee.

OPM’s OF-306 Accept Guidelines explain what must be shown in each block to ensure proper form completion for form OF-306. If this form is not properly coded, the Sponsor photocopies and returns the form(s). If the OF-306 is not properly completed, photocopy and return the form(s) to the Sponsor. USDA’s Personnel and Document Security Division’s (PDSD) internal checklist can be used as a transmittal memo to inform the Sponsor what corrections are needed. Agencies should modify the checklist to suit their needs.

### 2.2.3.2 Possible Disqualifying Information

The Sponsor will contact the Federal Employee/ Non-Federal Employee to discuss potentially disqualifying information. Examples of potentially disqualifying information include, but are not limited to:

- Use, possession, supply, or manufacture of illegal drugs in the last year.
- Conviction, imprisonment, probation, or parole during the last 10 years (includes felonies, firearms or explosive violations, misdemeanors, and all other offenses). (See Q9 on the OF-306).
- Conviction by military court-martial in the past 10 years. (See Q10 on the OF-306).
- Currently under charges for any violation of law. (See Q11 on the OF-306).
- Fired from any job during the last 5 years. (See Q12 of the OF-306 for conditions involving separation from employment that must be reported.)
- Current delinquency on any Federal debt. (See Q13 on the OF-306 for a specific explanation of the kind of delinquencies that must be reported.)

### 2.2.3.3 FBI Fingerprint Check

An FBI Finger Print (FP) Check is the minimum Background Investigation (BI) that must be performed for all applicable Federal Employees and Non-Federal Employees who require an AltLinc PIV-I credential as determined by the Risk Assessment. Agencies can leverage an existing FBI FP check or higher BI investigation if they have one on file AND the temporary employee has less than 1 year break in service. (Note: existing FBI FP checks should be no more than 120 days old). Otherwise, a new FP check must be completed.

Please note that USDA recommends that agencies process fingerprints electronically vs. a paper-based processing to improve efficiency and processing timeframes.

Agency human resources offices can meet the above requirement by completing the SF-75, Request for Preliminary Employment Data, Section K, Security Data, for Federal Employees transferring to the Department.

**\*\*Note:** All participants are subject to a finger print check before an AltLinc Card is processed. However, for those States who allow students to be hired and work at the age of 16 and do not have restrictions in place that will prevent them from obtaining an FBI Fingerprint check, the age restriction will be set to age 16. For those systems that require a security clearance or a high security (classified) system, they must have the appropriate background check (i.e NACI/ Tier-1 (Low Risk)) – based on the system requirements.

INTERIM

## Appendix A Definitions and Acronyms

### A-1 – Definitions

Term	Description
Adjudicator	A Government Employee of the sponsoring agency who resolves any issues or failures of the background check process and authorizes or denies the printing of a PIV credential.
Agency Role Administrator	The Agency Role Administrator is the individual responsible for managing the agency's sponsors, adjudicators, and Security Officers. The Agency Role Administrator will verify that the appropriate separation of role policies are followed and will verify that all the training certification requirements have been met.
AltLinc	PIV-I credential system for seasonal Federal employees and seasonal non-Federal employees with 6 months of employment for limited 2-factor logical and physical access to USDA IT systems and facilities.
Employee/ Non-Federal Employee	The Federal Employee/ Non-Federal Employee may be a current or prospective Federal hire, a Federal Employee, a Contractor Employee, or an Affiliate.
Biometric	A measurable physical characteristic used to recognize the identity of an individual. Examples include fingerprints, and facial images. A biometric system uses biometric data for authentication purposes.
Credential	Evidence attesting to one's right to credit or authority; in this standard, it is the AltLinc Credential and data elements associated with an individual that authoritatively binds an identity (and, optionally, additional attributes) to that individual.
EmpowHR	One of USDA's authoritative HR systems from which Employee Employee/ Non-Federal Employee data will be prepared and submitted to the USDA infrastructure.
e-QIP	The Electronic Questionnaires for Investigations Processing is an Office of Personnel Management (OPM) system that allows for the secure transmission of security questionnaires between government agencies and OPM.

Term	Description
FIPS 201-1	Federal Information Processing Standard (FIPS) 201, entitled Personal Identity Verification of Federal Employees and Contractors, was developed to satisfy the requirements of HSPD 12, approved by the Secretary of Commerce, and issued on February 25, 2005. FIPS 201 and accompanying special publications provide the standard for common identification by providing the requirements for the PIV smart card and its interfaces
HSPD-12	Homeland Security Presidential Directive 12 (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and Contractors," dated August 27, 2004
Identity Management System (IDMS)	One or more systems or applications that manage the identity verification, validation, and credential issuance process.
LincPass	USDA has named their common ID credential the LincPass, as it is designed to link a person's identity to an identification credential and the credential to a person's ability to access Federal buildings and computer systems. The spelling of LincPass is a tribute to President Abraham Lincoln, who created the People's Department (now USDA) in 1862.
Logical Access Control System (LACS)	Protection mechanisms that limit users' access to information technology (IT) systems by restricting their form of access to those systems necessary to perform their job function. These LACS may be built into an operating system, application, or an added system.
National Agency Check with Inquiries (NACI) or Tier-1 (Low Risk)	The basic and minimum investigation required of all Federal Employees, Contractor Employees, and Affiliates consisting of searches of the OPM Security/ Suitability Investigations Index (SII), the Defense Clearance and Investigations Index (DCII), the Federal Bureau of Investigation (FBI) Identification Division's name and fingerprint files, and other files or indices when necessary. A NACI/ Tier-1 (Low Risk) also includes written inquiries and searches of records covering specific areas of an individual's background during the past five years (inquiries sent to current and past employers, schools attended, references, and local law enforcement authorities).
National Criminal History Check (NCHC)	Fingerprint check portion of the background investigation
Payroll Personnel	One of USDA's authoritative HR systems from which Employee Employee/ Non-Federal Employee data will be prepared and submitted to the USDA infrastructure.

Term	Description
Person Model	USDA's secure and authoritative database for USDA identities and Non-Federal Employee information required by HSPD-12. Person Model feeds Non-Federal Employee information to EEMS (Enterprise Entitlements Management Service) which updates both USAccess (the General Services Administration (GSA) credentialing system).
U.S. Office of Personnel Management (OPM)	OPM is responsible for coordinating the FBI fingerprint check (FP Check), when applicable, and conducting the NACI/ Tier-1 (Low Risk) background investigation (BI).
Personal Identity Verification (PIV)	Personal Identify Verification (PIV) is the term designated in FIPS 201 for the processes and technologies involved in (a) identification: verifying the identity of a Federal employee or contractor at the time of initial identification and enrollment into a Federal agency's identity management system, and (b) authentication: verifying the identity of the Federal Employee or contractor for purposes of physical and information systems access control
Physical Access Control System (PACS)	Protection mechanisms that limit users' access to physical facilities or areas within a facility necessary to perform their job function. These systems typically involve a combination of hardware and software (e.g., a card reader), and may involve human control (e.g., a security guard).
Sponsor	The individual who substantiates the need for a PIV or PIV-I credential to be issued to a Federal Employee/ Non-Federal Employee, enters the Federal Employee's/ Non-Federal Employee's required sponsorship data elements into the system, and remains aware of the Federal Employee's/ Non-Federal Employee's status and continuing need for holding a PIV credential.
Security Officer	Security Officer is the individual responsible for maintaining credential security as well as physical building security for their agency.
Standard Form (SF)-85	Questionnaire for Non-Sensitive Positions
Standard Form (SF)-85P	Questionnaire for Public Trust Positions
Standard Form (SF)-86	Questionnaire for National Security Positions
Standard Form (SF)-87	Fingerprint Chart used to conduct FBI fingerprint checks for Federal appointees and Employees and Federal Employee/ Non-Federal Employees for federal employment
USAccess	Shared service solution offered by GSA MSO to issue HSPD-12 compliant ID credentials

Term	Description
USDA Credential Matrix/Risk Assessment	The determination of a person's legitimate need for physical/logical access using a PIV ID credential as outlined in HSPD-12 to USDA facilities/information systems, and the requirement to view sensitive information.
USDA Role Administrator	USDA Role Administrator assigns Agency Role Administrator roles within USDA.

*Table 2: Definitions*

## A-2 - Acronyms

Acronym	Definition
ACL	Access Control List
AltLinc	Personal Identity Verification, Alternate
BI	Background Investigation
CA	Certification Authority
CHUID	Cardholder Unique Identifier
CMS	Card Management System
DM	Departmental Manual
DR	Departmental Regulation
e-QIP	Electronic Questionnaires for Investigations Processing
FBI	Federal Bureau of Investigation
FBI Fingerprint Check	FBI National Criminal History Fingerprint Check
FIPS 201-1	Federal Information Processing Standard Publication 201-1
GSA	General Services Administration
HR	Human Resources
HRSD	Human Resources Service Division
HSPD-12	Homeland Security Presidential Directive 12
IDMS	Identity Management System
LACS	Logical Access Control System
NAC	National Agency Check
NACI	National Agency Check with Inquiries
NCR	National Capital Region
NIST	National Institute for Standards and Technology

Acronym	Definition
OCIO	Office of the Chief Information Office
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OPM/NS BI	Office of Personnel Management or National Security Community Background Investigation
OPPM	Office of Procurement and Property Management
OSS	Office of Security Services
PACS	Physical Access Control System
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification, Part I
PIV-II	PIV-II Personal Identity Verification, Part II
PDSD	Personnel and Document Security Division
PKI	Public Key Infrastructure
POC	Point of Contact
SF	Standard Form
SOI	Security Office Identifier
SON	Submitting Office Number
SP	Special Publication
SSP	Shared Services Process
USDA	United States Department of Agriculture

Table 3: Acronyms

## Appendix B Acceptable Enrollment ID List

<p><b>During the AltLinc credentialing process, you will need to validate your identity during the onboarding process as well as during card issuance. You must present two (2) acceptable forms of identification during the AltLinc Identity Establishment and Eligibility Process and the Issuance Process. One ID must be any one of items 1 through 5 in the list below (Primary ID). The other ID may be any of the forms if ID listed below (Primary or Secondary ID types).</b></p>	
<b>Primary Forms of Identification (Items 1 through 5)</b>	13. Certificate of Naturalization (Form N-550 or N570)
1. U.S. Passport (unexpired or expired)	14. U.S. Citizen ID Card (Form 1-197)
2. Driver's license or ID card issued by a state or possession of the United States provided it contains a photograph (unexpired)	15. Unexpired foreign passport, with I-551 stamp or attached Form I-94 indicating unexpired employment authorization
3. U.S. Military ID card (unexpired)	16. ID Card for use of Resident Citizen in the United States (Form I-179)
4. U.S. Military dependent's ID card (unexpired)	17. Permanent Resident Card or Alien Registration Receipt Card with photograph (Form I-151 or I-1551)
5. Department of Defense Common Access Card (CAC) (unexpired)	18. Certification of Birth Abroad issued by the Department of State (Form FS-545 or Form DS-1350)
<b>Secondary Forms of Identification (Items 6 through 25)</b>	19. Unexpired Temporary Resident Card (Form I-668)
6. U.S. Social Security Card issued by the Social Security Administration	20. Unexpired Employment Authorization Card (Form I-668-A)
7. Original or certified copy of a birth certificate issued by a state, county, municipal authority, or outlying possession of the United States bearing an official seal	21. Unexpired Reentry Permit (Form I-327)
8. ID card issued by federal, state, or local government agencies or entities, provided it contains a photograph	22. Unexpired Refugee Travel Document (Form I-571)
9. School ID with a photograph	23. Unexpired employment authorization document issued by DHS
10. Voter's registration card	24. Unexpired Employment Authorization Document issued by DHS with photograph (Form I-668-B)
11. U.S. Coast Guard Merchant Mariner card	25. Driver's license issued by a Canadian government authority
12. Certificate of U.S. Citizenship (Form N-560 or N-561)	26. Native American tribal document
<p>For example, the following are all acceptable combinations of ID that will successfully validate your identity:</p> <p>Example 1:</p> <p>a) Virginia State Driver's license (from Primary list, item 2)</p> <p>b) US Social Security Card (from Secondary list, item 5)</p> <p>Example 2:</p> <p>a) U.S. Passport (expired) (from Primary list, item 1)</p> <p>b) Maryland State Driver's license (from Primary list, item 2)</p> <p>Example 3:</p> <p>a) U.S. Military ID Card (from Primary list, item 3)</p> <p>b) Department of State ID Card (from Secondary list, item 7)</p>	

Figure 3: Acceptable Enrollment ID List